



УТВЕРЖДАЮ

Временно исполняющий обязанности

ФГБНУ ВНИИ «Радуга»

С.С. Турапин / С.С. Турапин

«15» 12 2025 г.

ПОЛОЖЕНИЕ О РЕАЛИЗУЕМЫХ ТРЕБОВАНИЯХ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (в редакции от 24.06.2025 г., далее – Закон № 152-ФЗ), иными нормативными правовыми актами Российской Федерации и устанавливает состав и содержание реализуемых Оператором – ФГБНУ ВНИИ «Радуга» (далее – Оператор) организационных и технических мер по защите персональных данных при их обработке.

1.2. Положение является неотъемлемой частью документа, определяющего политику Оператора в отношении обработки персональных данных, и подлежит опубликованию или обеспечению неограниченного доступа к нему в соответствии с частью 2 статьи 18.1 Закона № 152-ФЗ.

1.3. Требования настоящего Положения обязательны для исполнения всеми работниками Оператора, а также иными лицами, осуществляющими обработку персональных данных по поручению Оператора.

2. Перечень и описание организационных мер защиты персональных данных

Оператором реализуются следующие организационные меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом № 152-ФЗ:

2.1. Назначение ответственного за организацию обработки персональных данных.

- В соответствии со статьей 22.1 Закона № 152-ФЗ Оператором назначено лицо, ответственное за организацию обработки персональных данных. Данное лицо:

- Получает указания непосредственно от исполнительного органа Оператора и подотчетно ему.

- Осуществляет внутренний контроль за соблюдением Оператором и его работниками требований законодательства о персональных данных.

- Организует прием и обработку обращений и запросов субъектов персональных данных.

- Доводит до сведения работников положения законодательства и локальных актов по обработке персональных данных.

2.2. Разработка и ведение внутренней документации.

- Оператором изданы и поддерживаются в актуальном состоянии следующие документы:

- Политика в отношении обработки персональных данных.

- Настоящее Положение о реализуемых требованиях к защите.

- Локальные акты, определяющие для каждой цели обработки: категории и перечни обрабатываемых данных, категории субъектов, сроки обработки и хранения, порядок уничтожения данных.

- Регламенты по реагированию на инциденты безопасности.

- Документы, устанавливающие процедуры, направленные на предотвращение, выявление и устранение нарушений.

2.3. Обеспечение внутреннего контроля и аудита.

- Регулярно осуществляется внутренний контроль и/или аудит соответствия обработки персональных данных:

- Требованиям Закона № 152-ФЗ и принятых в соответствии с ним нормативных актов.

- Установленным требованиям к защите персональных данных.

- Внутренней политике и локальным актам Оператора.

2.4. Оценка вреда и соразмерность мер защиты.

- Оператор проводит оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона № 152-ФЗ. Принимаемые меры безопасности являются соразмерными выявленным рискам и потенциальному вреду.

2.5. Работа с персоналом.

- Все работники Оператора, непосредственно осуществляющие обработку персональных данных:
 - Ознакомлены с положениями законодательства Российской Федерации о персональных данных и требованиями к их защите под подпись.
 - Ознакомлены с документами, определяющими политику Оператора, и локальными актами.
 - Проходят необходимое обучение по вопросам защиты персональных данных.

3. Перечень и описание технических мер защиты персональных данных

Для обеспечения безопасности персональных данных при их обработке, в том числе в информационных системах персональных данных (ИСПДн), Оператором реализуются следующие технические меры:

3.1. Обеспечение защиты ИСПДн.

- Для каждой ИСПДн определены актуальные угрозы безопасности данных.
- Внедрены организационные и технические меры, необходимые для выполнения требований к защите персональных данных и обеспечения установленного Правительством РФ уровня защищенности.
 - Применяются средства защиты информации (СЗИ), прошедшие в установленном порядке процедуру оценки соответствия (сертификации).
 - Обеспечивается учет машинных носителей персональных данных.

3.2. Обнаружение и реагирование на инциденты.

- Осуществляется обнаружение фактов несанкционированного доступа к персональным данным.

- Реализованы меры по обнаружению, предупреждению и ликвидации последствий компьютерных атак на ИСПДн, а также по реагированию на компьютерные инциденты.

- Обеспечивается взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, включая информирование о компьютерных инцидентах, повлекших неправомерные действия с персональными данными.

3.3. Управление доступом и аудит.

- Установлены и соблюдаются правила доступа к персональным данным, обрабатываемым в ИСПДн.

- Обеспечивается регистрация и учет всех действий, совершаемых с персональными данными в ИСПДн (ведение журналов событий безопасности).

3.4. Восстановление и уничтожение данных.

- Обеспечена возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа.

- Уничтожение персональных данных осуществляется с применением СЗИ, в составе которых реализована функция уничтожения информации и которые прошли процедуру оценки соответствия.

3.5. Контроль эффективности мер.

- Проводится оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода ИСПДн в эксплуатацию и в процессе ее функционирования.

- Осуществляется постоянный контроль за принимаемыми мерами безопасности и уровнем защищенности ИСПДн.

4. Уведомление об инцидентах безопасности

4.1. В соответствии со статьей 21 Закона № 152-ФЗ, в случае выявления инцидента, повлекшего неправомерную или случайную передачу (предоставление, распространение, доступ) персональных данных, Оператор

обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор):

* В течение 24 часов – о факте инцидента, предполагаемых причинах, предполагаемом вреде и принятых мерах по устранению последствий.

* В течение 72 часов – о результатах внутреннего расследования инцидента.

5. Заключительные положения

5.1. Состав и содержание мер, указанных в настоящем Положении, являются достаточными для обеспечения выполнения Оператором обязанностей, предусмотренных Законом № 152-ФЗ.

5.2. Оператор вправе самостоятельно определять состав и перечень конкретных мер, инструментов и технологий в рамках установленных требований, если иное не предусмотрено законом.

5.3. Настоящее Положение пересматривается в случае изменения законодательства, технологий обработки, появления новых угроз безопасности или по решению ответственного лица/руководства Оператора.

5.4. Контроль за исполнением настоящего Положения возлагается на лицо, ответственное за организацию обработки персональных данных.